

# HIPAA&TRICARE

November 2003, No. 9

N e w s l e t t e r

Health Insurance Portability and Accountability Act



## HIPAA Security Working Integrated Project Team (WIPT)

**O**n February 13, 2003, the Department of Health and Human Services (HHS) Secretary, Tommy

Thompson, announced the adoption of the HIPAA security final rule. The final standards were published in the February 20 Federal Register with an effective date of April 21, 2003. Most covered entities will have two full years — until April 21, 2005 — to comply with the standards. This final rule adopts standards for the security of electronic protected health information to be implemented by health plans, health care clearinghouses, and certain health care providers. The use of the security standards will improve the effectiveness and efficiency of the health care industry by establishing a level of protection for electronic health information. The rule specifies a series of administrative, technical, and physical security procedures to assure the confidentiality of electronic protected health information.

As with the implementation of the HIPAA rules for Transactions and Code Sets and Privacy, the Military Health System (MHS) formed a Working Integrated Project Team (WIPT) for the HIPAA security rule. The HIPAA security WIPT is composed of representatives from the Air Force, Army, Navy, and Coast Guard, as well as the Lead Agent Office, TRICARE Regional Operations, and several other MHS Program Offices. The function of the WIPT is to employ a program planning approach to provide an implementation and compliance strategy for HIPAA security. This

methodology includes the following key functions: planning, policy, training and operations. Each sub-committee is lead by a Service representative and each WIPT member participates on one of the functional sub-committees and provides the perspective and input of the organization and service that they represent.

Planning Sub-Committee - The primary goal of this committee is to design, develop, implement, and monitor the MHS HIPAA Security Program. It will accomplish this goal through a measured, strategic process that integrates and coordinates the activities of the other sub-committees. The Planning Sub-Committee is chaired by representatives from the Army.

Policy Sub-Committee - The primary goal of this committee is to establish policy, responsibilities, procedures, and best practices that will ensure that DoD activities comply with HIPAA security requirements for protected information. This will be accomplished by developing a DoD HIPAA Security Regulation, a DoD HIPAA Security Handbook and HIPAA security implementation guides. The Policy Sub-Committee is chaired by representatives from the Navy.

Training and Awareness Sub-Committee - The primary goal of this committee is planning how to provide all members of the MHS workforce with annual HIPAA compliance training programs as well as provide all members of the MHS workforce with specific

### Inside This Issue . .

Security WIPT  
Overview



# HIPAA&TRICARE

November 2003, No. 9

N e w s l e t t e r

Health Insurance Portability and Accountability Act

HIPAA related responsibilities and additional training opportunities. The policies, procedures and responsibilities set forth by the HIPAA Security WIPT are integrated into an awareness campaign and addressed in an enterprise wide education and training plan. The Training and Awareness Sub-Committee is chaired by representatives from the Air Force.

Operations Sub-Committee – The primary goal of this committee is to establish an Oversight and Compliance Program that will report on the implementation of MHS HIPAA security at any point in time. This goal will be accomplished in several steps beginning with a baseline assessment of MHS HIPAA security practices and progressing through the development of several auditing and oversight plans. The Operations Sub-Committee is chaired by a representative of TMA regional operations.

This structure has been designed to enable MHS to address HIPAA security in an integrated and comprehensive manner. Moreover, the structure is designed to address any HIPAA security procedures shortcomings that may be identified and introduce implementation controls as required while ensuring support of mission requirements for each service.

Future activities of the HIPAA Security WIPT will be posted on the HIPAA security webpage (to be deployed December 2003) and included in updates to the HIPAA Newsletter. ■